ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION
EB Docket No. 06-36

Annual Section 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018.

1. Date filed: February 15, 2019

2. Name of company covered by this certification: Virginia Everywhere, LLC

3. Form 499 Filer ID: 831251

4. Name of signatory: James Carr

5. Title of signatory: CEO

6. Certification:

I, James Carr, certify that I am an officer of the company named above and, acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____,
James Carr, CEO

Attachment: Statement Explaining CPNI Procedures

CPNI POLICY STATEMENT

Use of CPNI and Safeguards

1. Our company utilizes an employee onboarding and training program to ensure compliance with CPNI rules and regulations.

2. Violations of the company's CPNI and other information security policies are subject to appropriate disciplinary action, up to and including termination.

3. All of the company's proprietary databases, including those containing customer information, are password protected, and access to the same is limited to authorized personnel only. Distribution of the passwords is limited to those authorized personnel. The passwords are changed routinely.

4. The company does not create or maintain any hard-copy customer files.

5. CPNI may not be removed from the company's offices by employees or others. This includes computer printouts, handwritten information or notes, copies of files or documents on a portable storage medium.

6. There is no verbal transmission of CPNI to persons who are not direct employees of the company.

7. Employees are required to closely guard customer lists, contact information, telephone numbers, and all other customer information, both proprietary and public, to prevent any information from being removed from our offices by non-employees either accidentally or intentionally.

8. Our company has a supervisory approval process in place for any proposed outbound marketing request for CPNI.

9. Our company does not have a retail presence, so there is no in-store access to CPNI.

10. Our company does not provide call detail information over the telephone.

11. Customers are authenticated before they are provided with access to our online portal. Once authenticated, a customer must provide a password to access its account information online.

12. Customer payments are processed by third party vendors through a PCI compliant system.

13. Notwithstanding the foregoing, it is the company's policy that the company may use, disclose or permit access to CPNI to protect the rights or property of the company, or to protect users of those services and other carriers from fraudulent, abusive or unlawful use of, or subscription to, such services.

Marketing

1. Our company does not conduct joint marketing with third parties.

2. The company does not and does not intend to use, disclose, or permit access to CPNI for marketing purposes. However, the company may, if applicable, use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.,* local, interexchange, and CMRS) to which the customer already subscribes from the company, without customer approval. If the company provides different categories of service, and a customer subscribes to more than one category of service offered by the company, the company is permitted to share CPNI among its affiliated entities that provide a service offering to the customer.

3. The company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

4. The company may, if applicable, use, disclose or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance and repair services.

5. The company, as a provider of interconnected VoIP services may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, called ID, call forwarding, and certain centrex features.

6. The company does not use, disclose or permit access to CPNI to market service offerings to a customer that require opt-in or opt-out consent of a customer under 47 C.F.R. § 64.2001 *et. seq.*

7. The company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

8. Notwithstanding the foregoing, it is the company's policy that the company may use, disclose or permit access to CPNI to protect the rights or property of the company, or to protect users of those services and other carriers from fraudulent, abusive or unlawful use of, or subscription to, such services.

9. The Company will properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online access, or in-store visit, if applicable, as described herein.

Law Enforcement and Customer Notice

1. Controls are in place involving responses to law enforcement agencies that serve our company with valid legal demands, such as a court ordered subpoena, for CPNI. Our

company will not supply CPNI to any law enforcement agency that does not produce a valid legal demand.

2. In the event of a breach, the company will not notify its customers or disclose the breach publicly until it has completed the process of notifying law enforcement.

3. As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the company will electronically notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") through a central reporting facility.

a. Notwithstanding any state law to the contrary, the company will notify customers or disclose the breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI, except as provided herein.

b. If the company believes that there is an extraordinary urgent need to notify any class of affected customers sooner than otherwise allowed hereunder, in order to avoid immediate and irreparable harm, it will so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The company will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

c. If the relevant investigating agency determines that public disclosure or notice to customer would impede or compromise an ongoing or potential criminal investigation or national security, the company will comply with such agency's written directives, including directives not to so disclose or notify for an initial period of up to thirty (30) days and extended periods as reasonably necessary in the judgment of the agency.

4. After the company has completed the process of notifying law enforcement pursuant hereto, it will notify its customers of a breach of those customers' CPNI.

5. The company will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant hereto, and notifications made to customers. The record will include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. The company will maintain the record for a minimum of two (2) years.